

Amendments to the Drawings:

In this response, Figs. 17 and 18 are submitted on substitute sheet. These figures have been amended to remove the "" (parenthesis) and "-" (dashes) therefrom. These amendments overcome the objections raised in connection with the drawings in paragraph #4 of this Office Action.

REMARKS

This is in full and timely response to the above-identified Office Action. The above listing of the claims replaces all prior versions, and listings, of claims in the application. Reexamination and reconsideration in light of the proposed amendments and the following remarks are respectfully requested.

Claims 1-7 are amended to clarify the subject matter which is set forth. These amendments at least overcome the rejection of claims 1-7 under 35 USC § 112 advanced in paragraphs 7-21 of this Office Action.

After amending the claims as set forth above, claims 1-7 are now pending in this application.

Claims 1-2 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Ueno et al. in view of Ichikawa et al. In addition, Claims 3-5 and 7 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Ueno et al. in view of Ichikawa et al. and in further view of Menezes et al. These rejections are both respectfully traversed.

In accordance with the claimed subject matter, the enciphering/deciphering program to be used for enciphering/deciphering a file to be transmitted, is directly determined by the electronic mail address of the send and the receiver. A reference table stored in the memory wherein the enciphering/deciphering program to be used is stored corresponds to the ordered pair relationship of the sender (transmission source electronic mail address) and the receiver (transmission destination electronic mail address). Upon enciphering (or deciphering), the reference table is looked up by using the transmission destination electronic mail address (or transmission source electronic mail address) as an index, automatically reads out the enciphering or deciphering program corresponding to the index data, and automatically enciphers (or deciphers) the target file.

This is made possible by storing the enciphering program and transmission destination data, deciphering program and transmission destination data, deciphering program and transmission source data, as corresponding data according to the ordered pair of the sender and the receiver. Such configuration is neither disclosed nor suggested in the cited references.

In the present invention, even if it is a communication (electronic mail transmission) between the same 2 person, for example between A and B, the enciphering program to be used and deciphering program to be used may change according to the direction of the transmission (whether the transmission is from A to B, or from B to A). This is because the enciphering program to be used is determined by the transmission destination electronic mail address, and depending on the direction of transmission, the destination electronic mail address changes. Therefore, the recipient of the transmission is free to select an enciphering program that he/she relies upon.

The Examiner admits that Ueno et al. (referred simply as Ueno hereinafter) do not teach using the designated transmission destination data (e-mail address) as a key for looking up the enciphering program in the reference table. The examiner further states that Ichikawa et al. (referred simply as Ichikawa, hereinafter) teach using the transmission destination data as a key 6 for looking up the enciphering program in the reference table. However, in Inchikawa, the transmission destination data corresponds to the "Terminal Address", as indicated in the col. 10, lines 30-55, of Ichikawa. The "terminal address" is utilized for comparing and basing the decision whether the wireless packet terminal is to be recognized as an authorized packet terminal or not.

Further, in Inchikawa col. 12, liens 42-52, it is stated that, "for sending a unicast packet, the wireless packet terminal 7-7 selects VLAN-key for encryption...In response to such key selection, if a unicast package is received...decodes the data packet using the terminal key, and if broadcast or multicast packet is received...decodes the data packet using the VLAN-key."

The above disclosure indicates that when receiving an encrypted data packet, by determining whether the data packet has been sent as a unicast or broadcast/multicast, the key to be used for decoding can be determined. In other words, there is only one key for unicast and one key for broadcast/multicast. There is no disclosure nor suggestion that indicates that a transmission source data is used for determining the deciphering program, as claimed in the present invention.

Further, as can be seen from the amended claims, the "transmission destination data" has been amended to "transmission destination electronic mail address" in order to indicated specific information that clearly determines the final destination (as disclosed in p.

3, 3rd paragraph of the specification). Also, "transmission source data" has been amended to "transmission source electronic mail address" for the same reason.

Further, according to the table 2 of Ichikawa, there is a column for storing the enciphering key as indicated by the Examiner. However, a deciphering program is not stored. In the present invention, the enciphering program has been pre-set to correspond to each transmission destination electronic mail address, and deciphering programs has been pre-set to correspond to each transmission source electronic mail address, and are stored in the reference table. In other words, two separate storing areas, a column for enciphering program and a column for deciphering program, are provided for a signal communication partner. This is neither disclosed nor suggested by the cited references.

In addition, in Ichikawa, col. 13, lines 21-23, it states that "all the packet terminals having the same VLAN-ID can decode broadcast or multicast packets." In Ichikawa, the terminal ID would be considered equivalent to the "transmission destination data" of the present invention, and it is what uniquely determines the final destination of the packet. However, the enciphering program is determined by the VLAN-ID and not by the terminal ID. Therefore, in Ichikawa, the enciphering program is not specified by looking up the reference table using the designated transmission destination data (electronic mail address) as a key. Thus, the enciphering program cannot be uniquely determined for each destination.

The claimed subject matter is such as to enable automatic determination of an enciphering program for each transmission destination, while allowing use of different enciphering programs for each destination. Therefore, a one-on-one relationship between the sender and the receiver, which creates the ordered pair, is the key to in the claimed arrangement. Such cannot be achieved by the disclosure of Ichikawa since the enciphered packet is designed to be decoded by more than one terminal. Thus, the claimed subject matter is distinctively different from that of the reference Ichikawa, and therefore the present invention cannot be considered obvious from Ichikawa even if combined with Ueno.

Claims 2-5 are dependent to Claim 1. As described above, Claim 1 is not obvious from the references. Therefore, these dependent claims are also not obvious in light of the cited references.

The Examiner has rejected claim 6 in that a voice signal is a file, and it would be obvious to extend Ueno and Ichikawa to a voice signal. The subject matter of Claim 6

corresponds to that of Claim 1, whereby all structural features of Claim 1 are represented by corresponding features associated with a telephone and the encryption of voice signal. Hence, the same argument as advanced in connection with Claim 1 above, is advanced with respect to Claim 6.

Claim 7 is a dependent claim depending on Claim 6. Therefore, the same argument advanced in connection with Claim 6 is also advanced in connection with Claim 7.

Applicant submits that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

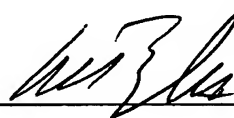
The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date

1/30/08

By



FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874

ANNOTATED SHEET

Title: Protected Communication System.

Inventor(s): Yasumasa Uyama

Appl. No.: 10/021,052

Atty. Docket No. 058856-0109

(a) the memory contents of Mr. S's telephone
the telephone No. of Mr. S is 0901111 . . .

destination (number)	enciphering key 1	enciphering key 2	deciphering key 1	deciphering key 2
0902222...	Yatottisotra...	Oaufefhgoo...	Abdefg...	Ynatnikatna...
0903333...	Y _a Y _B R _a Y _E W...	C _Y natmi _Y 1 _Y atra _Y ...	Jj _Y itso _Y k _Y ra _Y	Y _a Y _b Y _a Y _t Y _o ...

Fig. 17

(b) the memory contents of Mr. R's telephone
the telephone No. of Mr. R is 0902222 . . .

destination (number)	enciphering key 1	enciphering key 2	deciphering key 1	deciphering key 2
0901111...	Abcdefg...	Ynatnikatna _Y ...	Yatottisotra _Y ...	Oaufefhgoo...
0903333...	AaagggW...	A587XO...	4h3yg8jg85...	Xooo _Y na _Y R...

Fig. 18

voice	Kottnitchitwa (Hello) . . .
key 1	atotitsoraratotitsoraratotitsoraratotitsorara
key 2	hateetnathateetnathateetnathateetnathateetna

(a)

key 1	atituteotkataki (written in Japanese character) . . .	1,024 bytes
key 2	adfeohrorhohfo . . .	997 bytes
key 3	16467428744456 . . .	991 bytes

(b)